

Annual 47 C.F.R. § 64.2009(e) CPNI Certification for 2019 covering the prior calendar year 2018

1. Date filed: 02/12/2019
2. Name of company covered by this certification: Amicus Voice, LLC
3. Form 499 Filer ID: 0025876541
4. Name of signatory: Kerry Bohannon
5. Title of signatory: Owner

6. Certification:

I, Kerry Bohannon, certify that I am an officer of Amicus Voice, LLC ("Amicus Voice"), and, acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the customer proprietary network information ("CPNI") rules as set forth in Part 64, Subpart U of the Commission's rules, 47 C.F.R. §§ 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how Amicus Voice's procedures ensure that it is in compliance with the requirements (including those mandating the adoption of CPNI procedures, training, record keeping, and supervisory review) set forth in section 64.2001 *et seq.* of the Commission's rules.

Amicus Voice **has not** taken any actions (i.e., proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year.

Amicus Voice **has not** received customer complaints in the past year concerning the unauthorized release of CPNI.

I hereby represent and warrant that the above certification is consistent with 47 C.F.R. § 1.17 which requires truthful and accurate statements to the Commission, and acknowledge that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject Amicus Voice to enforcement action.



SignNow e-signature ID: 488c3c5f51...

02/12/2019 20:54:58 UTC

Kerry Bohannon

Owner and Compliance Manager

Amicus Voice, LLC

Executed 02/12/2019

Attachments: Accompanying Statement explaining CPNI procedures
 Explanation of actions taken against data brokers (if applicable)
 Summary of customer complaints (if applicable)

AMICUS VOICE STATEMENT OF POLICY REGARDING CPNI

In accordance with Section 222 of the Communications Act and the Federal Communications Commission's ("FCC") CPNI Rules (47 C.F.R. § 64.2001, et seq.), Amicus Voice, LLC ("Amicus Voice") files this Statement of Policy outlining the Company's procedures for accessing, using and storing Customer Proprietary Network Information ("CPNI").

Amicus Voice provides telecommunications services to retail customers. Because Amicus Voice may access, use, or store CPNI when providing these types of services, the Company undertakes the steps outlined in this Statement of Policy to protect CPNI from unauthorized access or misuse.

Definition of CPNI

Under federal law, CPNI is certain customer information obtained by a telecommunications provider during the course of providing telecommunications services (including interconnected VoIP) to a customer. This includes information relating to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier.

Examples of CPNI include information typically available from telephone-related details on a monthly bill such as the types of services purchased by a customer, numbers called, duration of calls, directory assistance charges, and calling patterns. CPNI does not include names, addresses, and telephone numbers, because that information is considered subscriber list information under applicable law.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

It is the policy of Amicus Voice not to use CPNI for any activity other than as permitted by applicable law. Any disclosure of CPNI to other parties (such as affiliates, vendors and agents) occurs only if it is necessary to conduct a legitimate business activity related to the services already provided by Amicus Voice to the customer. Except in instances where Amicus Voice is required by law to disclose CPNI, such as through subpoenas or other requests by law enforcement officials, or if the intended use is permitted by FCC Rules, Amicus Voice will first obtain the customer's consent prior to using or sharing CPNI.

Amicus Voice prohibits the release of CPNI based upon a customer-initiated telephone call except under the following three (3) circumstances:

- When the customer has pre-established a password;
- When the information requested by the customer is to be sent to the customer's address of record; or
- When Amicus Voice calls the customer's telephone number of record and discusses the information with the party initially identified by customer when service was initiated.

If Amicus Voice grants online access to CPNI, the Company authenticates a customer without the use of readily available biographical or account information prior to allowing the customer online access to CPNI stored online. Once authenticated, the customer may only obtain online access to CPNI through a password that is not prompted by the carrier asking for readily available biographical or account information.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

A. Password Authentication Procedures

To establish a password, Amicus Voice authenticates the identity of the customer without the use of readily available biographical or account information. If a customer cannot provide the correct password, the customer must establish a new password by contacting Amicus Voice or a Server Administrator with access to the customer's server, if the customer has designated a Server Administrator.

B. Account Change Notification

Amicus Voice notifies customers immediately of any account changes, including address of record, authentication, online account and password related changes. Each of the notices provided under this paragraph will not reveal the changed information and will direct the customer to notify Amicus Voice if they did not authorize the change.

C. Disclosure to Business Customers

Amicus Voice may negotiate alternative authentication procedures for services that the Company provides to business customers that have a dedicated account representative and a contract that specifically addresses the protection of CPNI.

D. Use of CPNI in Sales and Marketing Campaigns

Amicus Voice does not use CPNI in sales or marketing campaigns. For other uses, Amicus Voice will obtain prior approval and informed consent from its customers in accordance with the CPNI Rules for any similar use of CPNI. This will allow for the status of a customer's CPNI approval to be clearly established prior to the use of CPNI.

E. FCC Notification

Amicus Voice is prepared to provide written notice within five (5) business days to the FCC of any instance where the opt-in mechanisms do not work properly or to such a degree that consumers' inability to opt-in is more than an anomaly.

F. Third Party Use of CPNI

To safeguard CPNI, prior to allowing joint venturers or independent contractors access to customers' individually identifiable CPNI, Amicus Voice will require all such third parties to enter into a confidentiality agreement that ensures compliance with this Statement of Policy. Amicus Voice shall also obtain opt-in consent from a customer prior to disclosing the information to such third parties for marketing purposes. In addition, Amicus Voice requires all outside agents to acknowledge and certify that they may only use CPNI for the purpose for which that information has been provided.

Amicus Voice requires express written authorization from the customer prior to dispensing CPNI to new carriers, except as otherwise required by law.

Amicus Voice does not market or sell CPNI information to any third party.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

If an unauthorized disclosure of CPNI occurs, Amicus Voice shall provide notification of the breach within seven (7) days to the United States Secret Service ("USSS") and the Federal Bureau of Investigation ("FBI").

Amicus Voice will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI except as provided below. (A full business day does not count a business day on which the notice was provided.) Federal law requires compliance with this requirement even if state law requires disclosure.

If Amicus Voice receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Amicus Voice will delay notification to customers or the public upon request of the FBI or USSS. If the CPNI Compliance Manager believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customers; Amicus Voice still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

Notwithstanding the above, Amicus Voice shall not wait the additional seven (7) days to notify its customers if the Company determines there is an immediate risk of irreparable harm to the customers.

IV. RECORD RETENTION

Amicus Voice shall maintain records of discovered breaches for a period of at least two (2) years.

The CPNI Compliance Manager is responsible for assuring that we maintain for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Amicus Voice maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties or where third parties were allowed access to CPNI. If Amicus Voice later changes its policies to permit the use of CPNI for marketing, it will revise its record keeping policies to comply with the Commission's record keeping requirements.

Amicus Voice maintains a record of all customer complaints related to their handling of CPNI, and records of Amicus Voice's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that Amicus Voice considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Amicus Voice will have an authorized officer, as an agent of Amicus Voice, sign a compliance certificate on an annual basis stating that the officer has personal knowledge that Amicus Voice has established operating procedures that are adequate to ensure its compliance with FCC's CPNI rules. The certificate for each year will be filed with the FCC by the first business day or on after March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Amicus Voice's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

V. EMPLOYEE TRAINING POLICIES AND DISCIPLINARY PROCEDURES

All employees with access to CPNI receive a copy of Amicus Voice's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties. In addition, Amicus Voice requires CPNI training for all CSRs, personnel at retail offices that may receive requests for CPNI, and marketing personnel.

All employees of Amicus Voice are trained as to when they are, and are not, authorized to use CPNI. Through this training, Amicus Voice has informed its employees and agents that it considers compliance with the Communications Act and FCC Rules regarding the use, disclosure, and access to CPNI to be very important.

Violation by company employees or agents of such CPNI requirements will lead to disciplinary action (including remedial training, reprimands, unfavorable performance reviews, probation, and termination), depending upon the circumstances of the violation (including the severity of the violation, whether the violation was a first time or repeat violation, whether appropriate guidance was sought or received from a supervisor, and the extent to which the violation was or was not deliberate or malicious).

VI. ANNUAL CPNI CERTIFICATION

Pursuant to FCC regulations, 47 C.F.R. § 64.20089(e), Amicus Voice will annually submit to the FCC, prior to March 1st, a CPNI Certification of Compliance and accompanying Statement regarding the company's CPNI policies and operating procedures. These documents certify that Amicus Voice complied with federal laws and FCC regulations regarding the protection of CPNI throughout the prior calendar year. Individuals or entities that have questions about this CPNI Certification or the use of CPNI by Amicus Voice may contact the company's owner.

VII. CUSTOMER COMPLAINTS

Amicus Voice has not received any customer complaints in the past year concerning the unauthorized release of or access to CPNI.

VIII. ACTIONS TAKEN

Amicus Voice has not taken any actions against data brokers before state commissions, state or federal courts, or the FCC in the past year. Amicus Voice has no information, other than information that has been publicly reported, regarding the processes that pretexters are using to attempt to access CPNI.

Explanation of actions taken against data brokers

Not applicable for this past calendar year.

Summary of Customer Complaints

Not applicable for this past calendar year.

SignNow E-Signature Audit Log

Document name: CPNI 2018

Document ID: b6ad07e9ee447fb4b8cd84f4fcc46003dcc6a467

Document page count: 5

Client	Event	By	Server Time	Client Time	IP Address
SignNow Web Application	Uploaded Document	kb@amicusvoice.net	2019-02-12 08:53:27 pm UTC	2019-02-12 08:53:25 pm UTC	187.26.143.192
SignNow Web Application	Viewed the Document	kb@amicusvoice.net	2019-02-12 08:53:35 pm UTC	2019-02-12 08:53:35 pm UTC	187.26.143.192
SignNow Web Application	Document Saved	kb@amicusvoice.net	2019-02-12 08:54:12 pm UTC	2019-02-12 08:54:10 pm UTC	187.26.143.192
SignNow Web Application	Viewed the Document	kb@amicusvoice.net	2019-02-12 08:54:40 pm UTC	2019-02-12 08:54:40 pm UTC	187.26.143.192
SignNow Web Application	Signed the Document, Signature ID: 488c3c5f512823d27a07	kb@amicusvoice.net	2019-02-12 08:54:58 pm UTC	2019-02-12 08:54:57 pm UTC	187.26.143.192
SignNow Web Application	Added a Text	kb@amicusvoice.net	2019-02-12 08:54:58 pm UTC	2019-02-12 08:54:57 pm UTC	187.26.143.192
SignNow Web Application	Document Saved	kb@amicusvoice.net	2019-02-12 08:55:04 pm UTC	2019-02-12 08:54:57 pm UTC	187.26.143.192
SignNow Web Application	Added a Text	kb@amicusvoice.net	2019-02-12 08:55:04 pm UTC	2019-02-12 08:54:57 pm UTC	187.26.143.192